

SYSTEM AND METHOD USING INFORMATION BASED INDICIA FOR AUTHENTICATING TRANSACTIONS AND RECORDS

5 ABSTRACT OF THE DISCLOSURE

Method, system, and apparatus for authenticating transactions and records. A
nonce stamp is a physical article that is relatively difficult to copy illicitly, and that bears
a "nonce" number. The "nonce" is a relatively unique identifier, in that it is chosen from
10 a distribution such that any given user/customer is extremely unlikely to obtain two nonce
stamps bearing the same nonce. The method includes: presenting a nonce stamp having a
nonce number; presenting a numbered digital certificate derived securely from the nonce
number; and authenticating the transaction by comparing the number on the digital
certificate and the nonce number. The digital certificate is typically obtained by
15 users/customers in exchange for the purchase price of a desired transaction. The
apparatus is an information-based indicium including a nonce stamp, and a digital
certificate including a number derived securely from the nonce. The system generates
information-based transaction indicia, and typically includes one or more computers
configured to receive as input a nonce number from a user; encrypt the nonce number;
20 and provide to the user a digital certificate including the encrypted nonce number, so that
the nonce and the digital certificate may be collectively presented as an information-
based transaction indicium to authenticate a transaction..

004080-EGT-990